NBS TECHNICAL NOTE 906

U.S. DEPARTMENT OF COMMERCE / National Bureau of Standards

A Methodology for Evaluating Alternative Technical and Information Management Approaches to Privacy Requirements

QC
100
.U5753
NO.906
1976
C.2

NATIONAL BUREAU OF STANDARDS

The National Bureau of Standards [1] was established by an act of Congress March 3, 1901. The Bureau's overall goal is to strengthen and advance the Nation's science and technology and facilitate their effective application for public benefit. To this end, the Bureau conducts research and provides: (1) a basis for the Nation's physical measurement system, (2) scientific and technological services for industry and government, (3) a technical basis for equity in trade, and (4) technical services to promote public safety. The Bureau consists of the Institute for Basic Standards, the Institute for Materials Research, the Institute for Applied Technology, the Institute for Computer Sciences and Technology, and the Office for Information Programs.

THE INSTITUTE FOR BASIC STANDARDS provides the central basis within the United States of a complete and consistent system of physical measurement; coordinates that system with measurement systems of other nations; and furnishes essential services leading to accurate and uniform physical measurements throughout the Nation's scientific community, industry, and commerce. The Institute consists of the Office of Measurement Services, the Office of Radiation Measurement and the following Center and divisions:

Applied Mathematics — Electricity — Mechanics — Heat — Optical Physics — Center for Radiation Research: Nuclear Sciences; Applied Radiation — Laboratory Astrophysics [2] — Cryogenics [2] — Electromagnetics [2] — Time and Frequency [2].

THE INSTITUTE FOR MATERIALS RESEARCH conducts materials research leading to improved methods of measurement, standards, and data on the properties of well-characterized materials needed by industry, commerce, educational institutions, and Government; provides advisory and research services to other Government agencies; and develops, produces, and distributes standard reference materials. The Institute consists of the Office of Standard Reference Materials, the Office of Air and Water Measurement, and the following divisions:

Analytical Chemistry — Polymers — Metallurgy — Inorganic Materials — Reactor Radiation — Physical Chemistry.

THE INSTITUTE FOR APPLIED TECHNOLOGY provides technical services to promote the use of available technology and to facilitate technological innovation in industry and Government; cooperates with public and private organizations leading to the development of technological standards (including mandatory safety standards), codes and methods of test; and provides technical advice and services to Government agencies upon request. The Institute consists of the following divisions and Centers:

Standards Application and Analysis — Electronic Technology — Center for Consumer Product Technology: Product Systems Analysis; Product Engineering — Center for Building Technology: Structures, Materials, and Life Safety; Building Environment; Technical Evaluation and Application — Center for Fire Research: Fire Science; Fire Safety Engineering.

THE INSTITUTE FOR COMPUTER SCIENCES AND TECHNOLOGY conducts research and provides technical services designed to aid Government agencies in improving cost effectiveness in the conduct of their programs through the selection, acquisition, and effective utilization of automatic data processing equipment; and serves as the principal focus within the executive branch for the development of Federal standards for automatic data processing equipment, techniques, and computer languages. The Institute consists of the following divisions:

Computer Services — Systems and Software — Computer Systems Engineering — Information Technology.

THE OFFICE FOR INFORMATION PROGRAMS promotes optimum dissemination and accessibility of scientific information generated within NBS and other agencies of the Federal Government; promotes the development of the National Standard Reference Data System and a system of information analysis centers dealing with the broader aspects of the National Measurement System; provides appropriate services to ensure that the NBS staff has optimum accessibility to the scientific information of the world. The Office consists of the following organizational units:

Office of Standard Reference Data — Office of Information Activities — Office of Technical Publications — Library — Office of International Relations — Office of International Standards.

---

[1] Headquarters and Laboratories at Gaithersburg, Maryland, unless otherwise noted; mailing address Washington, D.C. 20234.

[2] Located at Boulder, Colorado 80302.

NATIONAL BUREAU OF STANDARDS
LIBRARY
JUL 7 1976
not 232

A Methodology for Evaluating Alternative Technical and Information Management Approaches to Privacy Requirements

t. Technical Note no 900

Robert C. Goldstein
Henry H. Seward, and
Richard L. Nolan

D. P. Management Corporation
1 Militia Drive
Lexington, Massachusetts 02173

Prepared for the
Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, D.C. 20234

U.S. DEPARTMENT OF COMMERCE, Elliot L. Richardson, *Secretary*

Dr. Betsy Ancker-Johnson, *Assistant Secretary for Science and Technology*

NATIONAL BUREAU OF STANDARDS, Ernest Ambler, *Acting Director*

Issued June 1976

National Bureau of Standards Technical Note 906

Nat. Bur. Stand. (U.S.), Tech. Note 906, 72 pages (June 1976)

CODEN: NBTNAE

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1976

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402
(Order by SD Catalog No. C13.46:906). Price $1.35 . (Add 25 percent additional for other than U.S. mailing).

Preface

The work presented on these pages represents, to our knowledge, a uniquely concrete and objective approach to evaluating some of the economic considerations resulting from the Privacy Act of 1974 (PL 93-579). By using a computer model to simulate the cost impact of the Act's requirements, one can determine the differences resulting from alternative approaches to implementing the mandated safeguards.

The computer model and the methodology it represents can be altered and modified to reflect changing circumstances and different record keeping systems. The publication of this work reflects our desire to improve the model by soliciting comments and suggestions from those involved in dealing with the task of complying with the law. By acting as a central collection point for these comments, NBS can provide a pool of knowledge that will aid all agencies.

Table of Contents

		Page
1.	Introduction	2
	1.1 Purpose	2
	1.2 Scope	3
	1.3 Privacy Act Requirements	3
	1.4 Methodology	6
	1.5 Guide to the Reader	8
2.	Act Requirements and Compliance Steps	10
	2.1 Requirement 1: Controlling Disclosure of Data	10
	2.1.1 Compliance Step 1	12
	Obtaining Consent for Additional Uses of Data	
	2.1.1.1 Action Steps (A-1 - A-5)	
	2.1.1.2 Algorithms	
	2.1.2 Compliance Step 2	15
	Check Consent Has Been Obtained	
	2.1.2.1 Action Steps (A-6 - A-10)	
	2.1.2.2 Algorithms	
	2.1.3 Compliance Step 3	16
	Claim Dissemination	
	2.1.3.1 Action Steps (A-11 - A-14)	
	2.1.3.2 Algorithms	17
	2.1.4 Compliance Step 4	18
	Retroactive Claim Dissemination	
	2.1.4.1 Action Steps (A-15 - A-17)	
	2.1.4.2 Algorithms	19
	2.2 Requirement 2: Accounting for Disclosures	20
	2.2.1 Compliance Step 5	20
	Maintain Usage Log	
	2.2.1.1 Action Steps (A-18 - A-21)	
	2.2.1.2 Algorithms	22
	2.2.2 Compliance Step 6	23
	Record Uses Inquiry	
	2.2.2.1 Action Steps (A-22 - A-24)	
	2.2.2.2 Algorithms	
	2.2.3 Compliance Step 7	24
	Legal Process Notification	
	2.2.3.1 Action Steps (A-25 - A-26)	
	2.2.3.2 Algorithms	
	2.3 Requirement 3: Access to Records	24
	2.3.1 Compliance Step 8	25
	Record Existence Inquiries	
	2.3.1.1 Action Steps (A-27 - A-31)	
	2.3.1.2 Algorithms	

Page

2.3.2 Compliance Step 9 27
Data Accuracy Inquiries
2.3.2.1 Action Steps (A-32)
2.3.2.2 Algorithms 28

2.3.3 Compliance Step 10 28
Claim Storage
2.3.3.1 Action Steps (A-33 - A-34)
2.3.3.2 Algorithms

2.4 Requirement 4: General Agency Requirements 29

2.4.1 Compliance Step 11 31
Data Accuracy
2.4.1.1 Action Steps (A-35 - A-39)
2.4.1.2 Algorithms

2.4.2 Compliance Step 12 33
Additional Data
2.4.2.1 Action Steps (A-40 - A-41)
2.4.2.2 Algorithms

2.4.3 Compliance Step 13 33
Revise Data Collection Forms
2.4.3.1 Action Steps (A-42 - A-43) 34
2.4.3.2 Algorithms

2.4.4 Compliance Step 14 34
Physical Security

2.4.4.1 Action Steps (A-44 - A-47)
2.4.4.2 Algorithms 35

2.4.5 Compliance Step 15 35
Training
2.4.5.1 Action Steps (A-48 - A-51)
2.4.5.2 Algorithms 36

2.4.6 Compliance Step 16 36
Audit
2.4.6.1 Action Steps (A-52 - A-55)
2.4.6.2 Algorithms 37

2.4.7 Compliance Step 17 37
Public Notice
2.4.7.1 Action Step (A-56)
2.4.7.2 Algorithms

3. Summary 38

Page

Table 1. 1974 Privacy Act Requirements and Compliance Steps 5

Table 2. Relationship of Privacy Act Requirements, Compliance Steps, Resources Required, and Dollars 7

Table 3. Requirement 1, Obtain Consent, Control Disclosure, Disseminate Claims 11

Table 4. Requirement 2, Accounting for Data Disclosures 21

Table 5. Requirement 3, Access to Records 26

Table 6. Requirement 4, General Agency Requirements 30

Appendix 1 Glossary of FORTRAN Variables 39

Appendix 2 Patterned Interview Format for Data Gathering 47

A METHODOLOGY FOR EVALUATING ALTERNATIVE TECHNICAL AND INFORMATION MANAGEMENT APPROACHES TO PRIVACY REQUIREMENTS

Robert C. Goldstein, Henry H. Seward,
Richard L. Nolan

ABSTRACT

Cost becomes an early concern in applying privacy safeguards to any computerized record-keeping system. To determine privacy cost impact one requires a concrete and rigorous approach that permits repeated analysis of carefully documented assumptions. Such a methodology appears in the work reported in the book The Cost of Privacy by Dr. Robert C. Goldstein. This report represents the application of that methodology to the technical requirements flowing from the Privacy Act of 1974 (PL 93-579).

The methodology presented reduces the legislation to 17 compliance steps. Each compliance step then decomposes into one or more specific actions required of the record-keeper. The actions, in turn, translate into the expenditure of different resources. The resources, in dollars, are computed by a set of algorithms collectively called a privacy model and implemented as a computer program.

The privacy model contains algorithms reflecting resource expenditures for 56 distinct actions. Written as a FORTRAN program, the model produces several printouts that show the user the consequences of the input data. In addition to a total cost for conversion and an annual operating cost, the model provides sub-total costs for each compliance step. The model's potential uses include the comparison of costs associated with alternative safeguards, the selection of an

optimal set of cost-effective safeguards, and the analysis of those factors having the greatest impact on costs.

KEY WORDS: Computer security; confidentiality; cost model; data security costs; PL 93-597; privacy; Privacy Act of 1974; privacy compliance techniques; privacy costs; privacy model; security costs.

1. INTRODUCTION

1.1 Purpose

This document presents a logical, structured method for evaluating alternative technical and information management approaches for compliance with the Privacy Act of 1974. Federal agencies must comply with this law after September 27, 1975. The structured approach described in this document will allow each agency to determine its own optimum compliance techniques by:

a. identifying actions which must be taken to comply, and

b. estimating the cost of these actions to see if low cost techniques are being utilized.

Planning for compliance may thus be based on a more substantive position.

1.2 Scope

The contents of this document represent an extension of earlier research conducted by Dr. Robert C. Goldstein and Dr. Richard L. Nolan at the Harvard Graduate School of Business Administration. Their previous research, which focused on the general implications of cost and implementation associated with privacy regulations, has been refined to reflect the 1974 Privacy Act and its specific requirements for Federal personal data bases. For the purpose at hand, "personal data base" is defined to be:

> a data base containing data on specific individuals and a set of application programs to manipulate this data in a manner in which the individual remains identifiable.

The model has been applied to three representative Federal personal data bases to estimate the costs of complying with the Privacy Act of 1974. Results have led us to believe that it is effective in selecting low cost compliance techniques.

1.3 Privacy Act Requirements

The Privacy Act establishes four specific sets of requirements:

(1) Obtain disclosure consent from the data subject before disseminating any information about the subject. Insure adequate steps have been taken to control disclosures.

(2) Maintain an accounting of disclosure and inform the affected individual concerning these disclosures upon an inquiry.

(3) Allow an individual access to records and a right to amend records.

(4) Maintain accurate data, provide physical security, train system users, audit-compliance, give public notice concerning the data base, and insure the individual is aware of use and disclosure rights when data is collected.

These requirements are summarized in Table 1 along with agency compliance steps for meeting requirements. An analysis of the resources required to implement these steps provides the underlying basis for cost estimation used in the Cost of Privacy Model.

The ordering in Table 1 is not prioritized. Different compliance techniques will have varying levels of applicability for different agency personal data bases. For example, if an agency is already maintaining a secure facility, little, if any, additional activity will be necessary to meet the physical security requirement. If procedures already exist to provide access to data, little additional

Table 1. 1974 Privacy Act Requirements and Compliance Steps

	Requirement*	Compliance Steps
1	Control Disclosure, Obtain Consent for Additional Use	1. Obtain consent for additional use of data from data subject 2. Check data subject consent prior to data dissemination 3. Disseminate subject claims 4. Disseminate retroactive claims
2	Accounting of Disclosures	5. Maintain usage log for personal data 6. Record uses inquiries 7. Provide notice of compulsory disclosure notification
3	Access to Records	8. Accommodate record existence inquiry 9. Accommodate data accuracy inquiry 10. Store subject claims
4	General Agency Requirements	11. Maintain data accuracy 12. Provide additional data if necessary 13. Design forms for data supply obligation notification 14. Provide physical security 15. Provide user and staff training 16. Audit for system assurance 17. Issue public notice

*Subsections of Title 5, United States Code, Section 552a

effort will be necessary to satisfy the Act in this area. The cost model provides an estimate of the "incremental cost" to be incurred by a Federal Agency in complying with the Privacy Act of 1974.

1.4 Methodology

Our approach has four major components (summarized in Table 2):

(1) General requirements of the Privacy Act of 1974 are described at a detailed level of definition (referred to as "compliance steps").

(2) Specific actions which an agency must take to implement these compliance steps are defined.

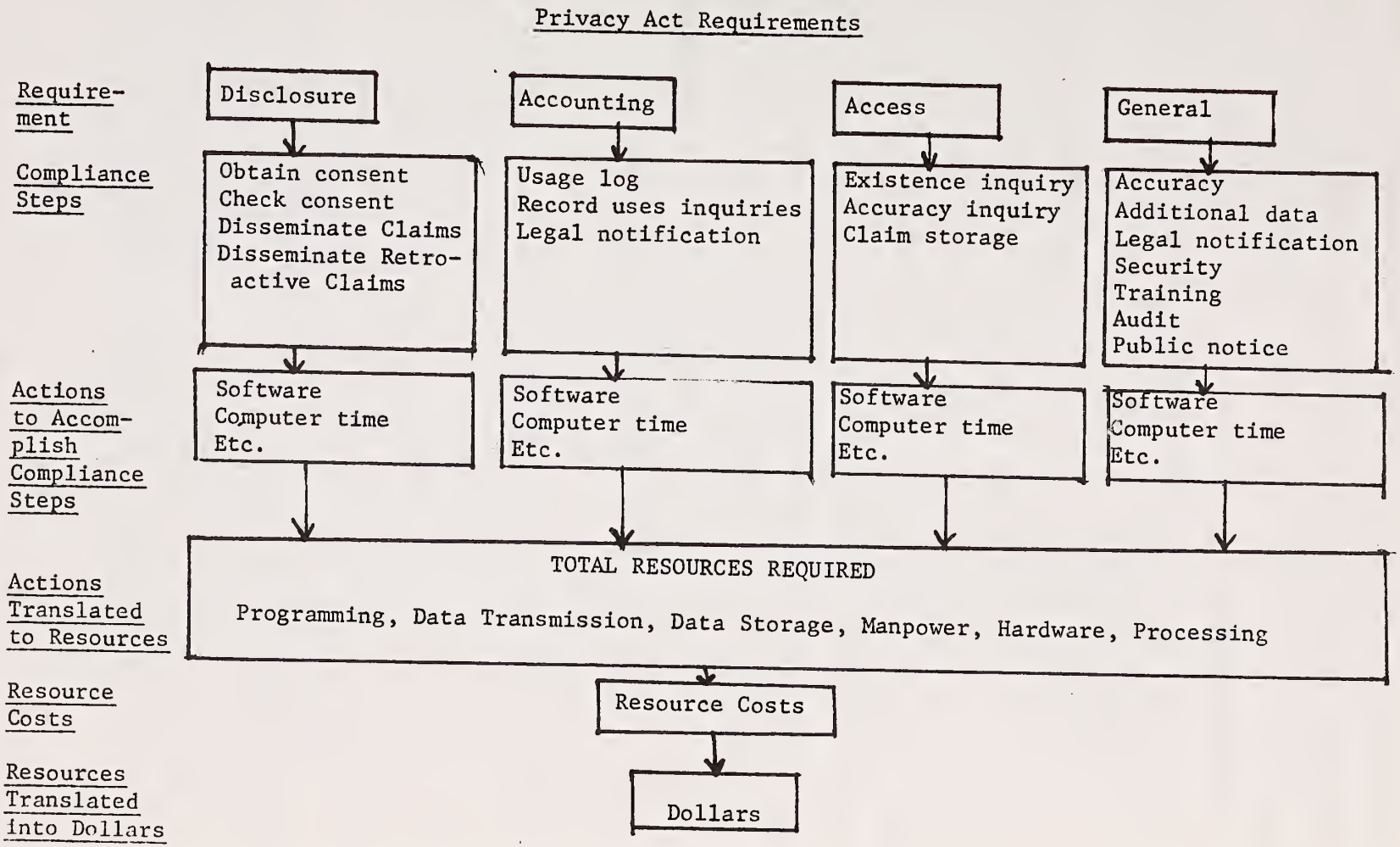
(3) Algorithms to estimate the resources of carrying out these actions are developed. Costs are then applied to these resources to determine dollars required for compliance.

(4) A methodology for gathering the necessary descriptive information about a specific Agency's data base (which serves as input to the Cost Estimation model) is defined.

The algorithms for estimating resources and cost have been derived from empirical experience in the initial definition of the model. In a number of cases, the specific actions implied by the algorithms represent the "least cost" approach to implementing the compliance step and are based on empirical evaluation of alternative actions which proved less costly. Thus, while this model does not presume to estimate the minimum cost of implementing the Act, a considerable amount of judgment derived from experience has been incorporated.

Similar informed judgment has been exercised in the definition of input data which drive the model. The nature of these informed judgments are described in this document. A critical component in

Table 2. Relationship of Privacy Act Requirements, Compliance Steps Resources Required, and Dollars



the effective application of our model is the sensitivity analysis of the final estimates to assumptions (informed judgments) concerning input parameters. Thus, reliable cost estimates can be derived only if sufficient effort is applied to controlling the reliability of input data, and maintaining an awareness of the effects of key judgments.

1.5 Guide to the Reader

Section 2 describes the four major requirements of the Privacy Act of 1974. For each of the requirements, an analytical procedure is specified for developing the algorithms of the model. First, based upon a general description of the four requirements from the Act, specific compliance steps to meet the requirements are defined, and are numbered sequentially. Second, specific actions necessary to meet the compliance step are defined. These actions are broken into two categories, nonrecurring and recurring, and are also numbered sequentially. Finally, algorithms for estimating the resources necessary to accomplish actions are defined.

Data about the personal data system under study is input to the algorithms of the model which, in turn, output incremental resources required for compliance with the Privacy Act. The resources are then multiplied by cost factors to provide a cost of compliance.

Judgment has been used in attributing actions to specific compliance steps. Some steps assume that certain other steps are also being accomplished. For example, the checking of access authorization prior to disclosing personal data assumes that a list of authorized

uses and recipients has been prepared based on the data subject's explicitly obtained consent. In addition, there are situations where a single action may facilitate implementation of more than one compliance step. Certain programming activities, for example, fall into this category. As an example, computer programming to handle the recording of data usage will also be used in answering record usage inquiries received from data base subjects. Care has been taken to ensure that all necessary actions have been included, and that none have been included more than once.

Another general point which relates to all the actions is that they have been chosen after considerable thought and review of many action alternatives. The selected actions discussed here, in our opinion,provide efficient technical compliance. They are efficient in the sense that they satisfy act requirements at a resource expenditure level which is reasonable when compared to possible alternatives.

The degree to which the suggested action is implemented is a management decision of the specific agency. As an example, Requirement 4 requires an agency to take adequate steps for physical security. Just how much physical security is needed must be decided by the agency. In the future, it is quite likely that the precise degree of security (and other steps) needed for personal data base compliance will be arrived at as a result of government agency implementation and government audit of these compliance implementations.

Appendix 1 contains a glossary of terms. Appendix 2 contains the Patterned Interview format for gathering data.

2. REQUIREMENTS, COMPLIANCE STEPS, AND ACTIONS TO MEET COMPLIANCE STEPS

2.1 Requirement 1: Controlling Disclosure of Personal Data

Requirement b of the Privacy Act states:

> No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the records pertain....

Certain requirements of d also relate to disclosure:

> d(4) in any disclosure, containing information about which the individual has filed a statement of disagreement (the agency will) clearly note any portion of the record which is disputed and provide copies of the (data subject's) statement...to persons or other agencies to whom the record has been disclosed.

The general exception to this clause relates to routine intra-agency use. Written permission is not needed in this case. Also, if the data is being disclosed to law enforcement agencies, the Privacy Act does not require disclosure to the data subject. Table 3 shows the actions necessary to meet the compliance steps related to Disclosure requirements: Compliance Steps 1-4

> 1. An agency must obtain written consent for additional uses of personal data from each data subject.
>
> 2. Prior to data disclosure, the agency must check that consent has been obtained.
>
> 3. If the subject disagrees with the data, and has filed a dissenting claim, this claim must also be forwarded to the person or agency receiving the data.
>
> 4. If a subject disagrees with the data, and has filed a dissenting claim, the agency must retroactively disseminate this claim to all previous persons or agencies to whom the data has been disclosed.

Table 3. Requirement 1, Obtain Consent, Control Disclosure, Disseminate Claims

Compliance Step	Actions Necessary to Accomplish Compliance Step
1. Obtain Consent for Additional Use of Data Subject	NONRECURRING A1 - Develop software to generate form letters to data subjects asking for consent to disseminate data-QUAN(2,1)* A2 - Develop software to record access control information on data subject's record and/or at data base level-QUAN(2,1) RECURRING A3 - Maintain software-QUAN(2,6) A4 - Operate computer to enter, maintain, and control information at individual record level-QUAN(2,9) A5 - Mail letters-QUAN(2,11)
2. Check Data Subject Specific Consent Prior to Data Dissemination	NONRECURRING A6 - Develop software to check data user identification to the system-QUAN(3,1) A7 - Develop software to check authorization for data use-QUAN(3,1) RECURRING A8 - Maintain software-QUAN(3,6) A9 - Operate computer to check usage-QUAN(3,8) or QUAN(3,7) A10 - Perform clerical effort if a clerical intermediary is used-QUAN(3,14)
3. Disseminate Subject Claims	NONRECURRING A11 - Develop software to retrieve claim information-QUAN(12,1) RECURRING A12 - Maintain software-QUAN(12,6) A13 - Operate computer to retrieve claim information-QUAN(12,10) or QUAN(12,9) A14 - Transmit data for claim if inquiry is online-QUAN(12,12)
4. Retroactively Disseminate Claims	RECURRING A15 - Operate computer to search usage log for past data recipients-QUAN(13,9) A16 - Perform clerical effort to notify past recipients-QUAN(13,14) A17 - Mail letters-QUAN(13,11)

*Name for action step in related algorithm

2.1.1 Compliance Step 1

An agency must obtain written consent for additional uses of personal data from each data subject.

2.1.1.1 Five actions (A-1 - A-5) are necessary to meet this compliance step.

A-1. Nonrecurring - Develop software to generate form letters to data subjects asking for consent to disseminate data.

A-2. Nonrecurring - Develop software to record access control information in the data subject's record.

A-3. Recurring - Maintain the software.

A-4. Recurring - Operate the computer to enter, maintain, and control disclosure of data.

A-5. Recurring - Send letters to obtain consent.

2.1.1.2 Algorithms for each of the above actions (Section 2.2.1.1) follow.

A-1 and A-2. Software (QUAN(2,1))

$$QUAN(2,1) = PNOT + PWAC$$

PNOT - The amount of programming time necessary to generate a program for writing form letters to all data subjects.

PWAC - The amount of programming time necessary to generate a program to permit the recording of all access control information within the data base and within each subject's record.

A-3. Software maintenance (QUAN(2,6))

$$QUAN(2,6) = PRGMNT * QUAN(2,1)$$

PRGMNT - the percentage of initial programming time required annually for program maintenance.

QUAN(2,1) - defined above

(FORTRAN notation is used. *equals multiplication.)

A-4. Computer Processing (QUAN(2,9))

QUAN(2,9)=NSUB*((1+FRPT)*(TCPU*(ISCN+IFRM))

+FOBJ*(.5*GET+TCPU*IWAC))*NNUS

NSUB - The number of individuals about whom identifiable personal data is stored in the system.

FRPT - The percentage of NSUB which will require follow-up letters to obtain consent.

ONLN - If the data base is online, ONLN=1. If the data base is offline, ONLN=0.

NREC - Total number of data subject records. It may be greater than NSUB as one individual may have more than one record in the data base.

SREC - Average number of characters in a record.

FOBJ - The percentage of data subjects who may be expected to object to a proposed new use for their information. If a subject objects, his record must be so annotated and blocked from use.

TCPU - Average time in seconds required to execute 1 instruction.

ISCN - The number of CPU instructions per record to scan a file.

IFRM - The number of CPU instructions to format a request to data subjects.

IWAC - The number of CPU instructions to write control access information.

NNUS - Number of new uses for the data base each year.

GET - Get is a function used by several of the algorithms to determine the time necessary to get a record from the file. There are four items used by the GET function (N,R,L,Q)

N=1 - The data base is online. If this is true GET = .14 seconds. This parameter may be varied if necessary.

N=0 if offline

R = Number of records in file

L = Length of record

Q = Number of records to be retrieved

If Q is less than or equal to one, one-half the file must be read and access equals

$$GET = \frac{R*L}{120,000}*.5$$

If Q is greater than 1 and N=0, the entire file must be read and

$$GET = \frac{R*L}{120,000}*Q$$

In this case GET(N,R,L,Q) is read as GET(ONLN, NREC, SREC, FOBJ*NREC)

The GET function is based on the following assumptions about file organization and usage:

a. Online data bases are assumed to be organized using the Indexed Sequential or equivalent method. Access to a single record, at random, will then require, on average, four disc accesses. A time of 35 milliseconds per access is used as being reasonably typical of today's high performance disc systems.

b. Offline files are assumed to be stored on tape using technology that permits reading the tape at a rate of 120,000 characters per second. If only one record is to be retrieved, one half the file must be read, on the average. If more than one record is to be retrieved during a single search, it is assumed that the entire file will be read and the total time allocated equally among all the records retrieved. 1/120,000 second is the amount of time to read one character in the file.

A-5. Send letters (QUAN(2,11))

QUAN(2,11) = (1.+FRPT+FOBJ)*NSUB

2.1.2 Compliance Step 2

Prior to data disclosure, the agency must check that consent has been obtained.

2.1.2.1 Five actions (A-6 - A-10) are necessary to meet this compliance step.

A-6. Nonrecurring - Develop software to check user identification to the system, i.e., is user authorized to query the system.

A-7. Nonrecurring - Develop software to check authorization for data use.

A-8. Recurring - Maintain software.

A-9. Recurring - Operate computer to check usage consent and access information.

A-10. Recurring - Utilization of clerical time if an intermediary is required.

2.1.2.2 Algorithms for each of the above actions (2.2.2.1) follow:

A-6 and A-7. Software (QUAN(3,1))

$$QUAN(3,1)=PUID + PACC*NDRP$$

PUID - the programming time required to add a user identification to the system.

PACC - the programming time to implement record level access control.

NDRP - the number of application programs which directly access the data base. NDRP=1 if a general data management system is used to handle all requests for data by applications programs.

A-8. Program Maintenance (QUAN(3,6))

$$QUAN(3,6) = PRGMNT*QUAN(3,1)$$

A-9. Operate Computer - two algorithms

Store Access Information

(QUAN(3,8) if online)
(QUAN(3,7) if offline)

$$QUAN(3,8) \text{ OR } QUAN(3,7) = 12*(NUST+NREC*NRLC)$$

12 - 12 characters must be stored for each data base level access (NUST) and for each record level access (NREC*NRLC)

NUST - the number of sets into which all users can be lumped for access control purposes

NRLC - the average number of record level access control fields per record. Required for those uses for which there is not a general data subject consent.

Perform Access Checks (QUAN(3,10) if online) (QUAN(3,9) if offline)

QUAN(3,10) OR QUAN(3,9) = NTRN*(GET+2*ICACL*TCPU)

NTRN - the average number of access transactions processed per year

(N) (R) (L)(Q)
GET (1,NUST,12,1) - previously defined

ICACL - the number of CPU instructions to check the access control list

A-10. Clerical Time (QUAN(3,14))

QUAN(3,14)=NTRN*HUID

HUID - The number of hours of clerical time required to confirm the identity of a person submitting an inquiry.

2.1.3 Compliance Step 3

If the subject disagrees with the data and has filed a dissenting claim, this claim must also be forwarded to the person or agency receiving the data.

2.1.3.1 Four action steps (A-11 - A-14) are necessary to accomplish this step.

A-11. Nonrecurring - Software to retrieve claim information.

A-12. Recurring - Maintain software.

A-13. Recurring - Operate Computer to retrieve claim information.

A-14. Recurring - Transmit data concerning claims (online systems)

2.1.3.2 Algorithms are as follows:

A-11. Software (QUAN(12,1))

QUAN(12,1)=PDCL*(1+0.1*(NRPR-1))

PDCL - the programming effort to modify a record retrieval program to include the claim field in its response to all inquiries.

NRPR - the number of record retrieval programs utilizing the data base.

.1(PDCL) - the additional effort necessary to modify subsequent retrieval programs after the first program has been modified.

A-12. Maintenance (QUAN(12,6))

QUAN(12,6)=PRGMNT*QUAN(12,1)

A-13. Operate Computer (QUAN(12,10) if online)

(QUAN(12,9) if offline)

QUAN(12,10) or QUAN(12,9)=NTRN*(NUDS*TRRT/NREC)*(SCLM/SREC)*TTRN

ISTR - a logical variable whose value is true if the system primarily processes structured inquiries and false if inquiries are primarily unstructured. Unstructured inquiries require greater amounts of transaction processing time.

SANS - size of the average inquiry answer.

TTRN - the computer time needed to process one transaction.

NTRN*(NUDS*TRRT/NREC)- number of transactions per year that will access records to which claims are attached.

(SCLM/SREC)*TTRN)- determines the additional computer time to process one claim.

TTRN=OPS*SANS*TCPU

OPS - the number of instructions which must be executed to produce each character of the answer.

OPS=100 if ISTR is true

OPS=300 if ISTR is false

NTRN - the average number of transactions processed by the system per year.

NUDS - the number of data accuracy inquiries that are not settled and must be added to the data base/year.

NUDS=(1-FRDS)*NDAI

FRDS - the percentage of data accuracy inquiries that will not result in the addition of a claim to the data base.

TRRT - number of years a record is retained.

SCLM - space needed to hold one subject's claim

A-14. Data transmission (QUAN(12,12))

QUAN(12,12)=(NUDS*TRRT/NREC)*NTRN*SCLM

2.1.4 Compliance Step 4

If a subject disagrees with the data, and has filed a dissenting claim, the agency must retroactively disseminate this claim to all previous persons or agencies to whom the data was disclosed.

2.1.4.1 Three actions (A-15 - A-17) are necessary to accomplish this compliance step.

A-15. Recurring - Operate computer to search usage log for past data recipients.

A-16. Recurring - Prepare form letter to past recipients.

A-17. Recurring - Mail claim to previous recipients.

2.1.4.2 Algorithms for these actions follow:

A-15. Search usage log (QUAN(13,9))

QUAN(13,9)=NDAI*GET

NLGS - the frequency of searching the usage log.

TLGR - number of years an entry is maintained in the usage log.

NREI - number of record existence inquiries per year.

NDAI - number of data accuracy inquiries per year.

FRUI - the fraction of record existence inquiries who will go on to inquire about the uses made of their record.

NRUI - number of record usage inquiries

NRUI=NREI*FRUI

```
    (N)  (R)      (L)              (Q)
GET (0, NREC, 20*NTRN*TLGR/NREC, NRUI+NDAI/NLGS)
```

See Section 2.3.2.2 for further comment.

A-16. Prepare form letters (QUAN 13,14)

QUAN (13,14) = HGSN*NDAI*(NTRN/NREC)*TLGR

HGSN - the amount of clerical time to prepare a standard notification.

Clerical time is based on the number of claims added to the file per year, NDAI, times the average number of transactions/record/year, times the average time the usage log is maintained.

A-17. Mail letters (QUAN(13,11))

QUAN(13,11) = NDAI*(NTRN/NREC)*TLGR

2.2 Requirement 2: Accounting for Personal Data Disclosures

Requirement c of the Privacy Act states:

> (1) Each agency...shall...keep an accurate accounting of (non-routine) disclosures.
>
> (a) the date, nature, and purpose of each disclosure of a record to any person or to another agency...
>
> (b) the name and address of the person to whom disclosure is made.
>
> (2) Retain the accounting made....for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made.
>
> (3)....make the accounting available to the individual named in the record at his request...
>
> (4) Inform any person or other agency about any correction or notation of dispute made by the agency. Also e(8)...serve notice when any record is made available under compulsory legal process when (it) becomes a matter of public record.

In order to accomplish this requirement, three compliance steps are necessary: Compliance Steps 5-7

> 5. The agency must maintain a usage log to record all disclosure to outside agencies.
>
> 6. The agency must inform the data subject about uses made of his personal data if the data subject makes a record uses inquiry.
>
> 7. If the agency discloses data as a result of a public legal process, it must notify the data subject.

2.2.1 Compliance Step 5

The agency must maintain a usage log to record all disclosures to outside agencies.

2.2.1.1 Four actions (A-18 - A-21) are necessary to maintain the usage log.

A-18. Nonrecurring - Develop software to implement the usage log capability.

A-19. Nonrecurring - Obtain a dedicated tape drive to store usage log entries.

A-20. Recurring - Maintain software.

A-21. Recurring - Operate computer to write and store usage log entries.

Table 4. Requirement 2, Accounting for Data Disclosures

Compliance Steps	Actions Necessary to Accomplish Compliance Step
5. Maintain Usage Log	NONRECURRING
	A18 - Develop software to implement the usage log capability QUAN(4,1)
	A19 - Obtain hardware dedicated to store entries QUAN(4,16)
	RECURRING
	A20 - Maintain software QUAN(4,6)
	A21 - Operate computer to write and store usage log entries QUAN(4,7) + QUAN(4,9) or (4,10)
6. Record Uses Inquiries	RECURRING
	A22 - Operate computer to respond to inquiries QUAN(7,9)
	A23 - Utilize clerical time to process inquiries QUAN(7,14)
	A24 - Mail Responses
7. Legal Process Notification	RECURRING
	A25 - Utilize clerical time to prepare notifications QUAN(16,14)
	A26 - Mail notification QUAN(16,11)

2.2.1.2 The following algorithms are used:

A-18. Software (QUAN(4,1))

QUAN(4,1)=PLOG

PLOG - the amount of programming time required to implement the usage log capability.

A-19. Hardware (QUAN(4,16))

QUAN(4,16)=KLOG

KLOG - the annual dollar cost of additional equipment needed to maintain the usage log.

A-20. Maintain Software (QUAN(4,6))

QUAN(4,6)=PRGMNT*QUAN(4,1)

A-21. Operate Computer (QUAN(4,7) + QUAN(4,10) if online)

(QUAN(4,7) + QUAN(4,9) if offline)

Storage (QUAN(4,7))

QUAN(4,7)=SLOG*NTRN*TLGR

SLOG - Size of a usage log entry

Write

Online (QUAN(4,10) + QUAN(4,9))

QUAN(4,10) = NTRN*TCPU*IWUL

QUAN(4,9) = 365*SORT(NTRN/365,SLOG)

QUAN(4,9) is a daily batch run to sort usage log entries by data subject. QUAN(4,10) initially stores transaction entries sequentially.

Offline

QUAN(4,9) = NTRN*TCPU*IWUL+365*SORT(NTRN/365,SLOG)

IWUL - Number of CPU instructions to write data in usage log.

SORT - A function whose value is the amount of computer time required to sort a file of X records of Y characters in length.

SORT(R,L) = R*L*.0000218

.0000218 - The average time to sort a character on representative high speed computers in seconds.

2.2.2 Compliance Step 6

The agency must inform the data subject about uses made of his personal data if the data subject makes a record uses inquiry.

2.2.2.1 Three actions (A-22 - A-24) are necessary.

A-22. Recurring - Operate the computer to respond to inquiries.
A-23. Recurring - Utilize clerks to process inquiries.
A-24. Recurring - Mail responses.

2.2.2.2 Algorithms are as follows:

A-22. Operate computer (QUAN(7,9))

QUAN(7,9)=NRUI*GET

	(N)	(R)	(L)	(Q)
GET	(0,	NREC,	(20*NTRN*TLGR/NREC),	(NRUI+NDAI)/NLGS)

Each usage log entry is assumed to contain 20 characters. It is assumed that after a data subject has made a record existence inquiry, he may or may not make a record usage inquiry. The agency will make computer runs periodically to answer these inquiries (NLGS). These periodic runs will also service data accuracy inquiries. The periodic computer runs must therefore be prorated between accuracy inquiries and usage inquiries.

A-23. Clerical time (QUAN(7,14))

QUAN(7,14)=HINQ*NRUI

HINQ - the clerical time necessary to process one inquiry.

A-24. Mailing effort (QUAN(7,11))

QUAN(7,11)=NRUI

2.2.3 Compliance Step 7

If the agency discloses data as a result of a public legal process, it must notify the data subject.

2.2.3.1 Two actions (A-25 - A-26) are necessary.

A-25. Recurring - Utilization of clerical time to prepare notifications.

A-26. Recurring - Mail notices

2.2.3.2 Algorithms

A-25. Clerical (QUAN(16,14))

QUAN(16,14)=NLPN*HGSN

NLPN - the number of legally enforceable requests for data received per year.

HGSN - clerical time to process a legal response

A-26. Mailing Effort (QUAN(16,11))

QUAN(16,11)=NLPN

2.3 Requirement 3: Access to Records

Requirement d of the Privacy Act states:

> Each agency that maintains a system of records shall: (1) Upon request by any individual to gain access to his record or to any information pertaining to him, permit him....to review the record and have a copy made...in a form comprehensible to him. (2) Permit the individual to request amendment of a record pertaining to him and (a) after....receipt of such a request, acknowledge in writing such receipt; and (b) promptly, either: (i) make any correction of any portion...which the individual believes is not accurate or (ii) inform the individual of its refusal to amend the record..., the reason for the refusal, the procedures established by the agency....to request a review.

Section d requires an agency to complete three compliance steps (8-10)

8. The agency must be able to respond to record existence inquiries from individuals.

9. The agency must be able to respond to data accuracy disputes,i.e., it must have the machinery to adjudicate disputes concerning data accuracy.

10. If a dispute is not resolved, the agency must store the subject's claim.

2.3.1 Compliance Step 8

The agency must be able to respond to record existence inquiries from individuals.

2.3.1.1 Five action steps (A-27 - A-31) are necessary to be able to respond to existence inquiries.

A-27. Nonrecurring - Develop software to permit retrieval of subject information.

A-28. Recurring - Maintain software.

A-29. Recurring - Process inquiries, using clerical personnel.

A-30. Recurring - Operate the computer to access and copy data.

A-31. Recurring - Mail the data to subjects.

2.3.1.2 Required algorithms

A-27. Software (QUAN(6,1))

If there is a data base management system (DBMS), only the DBMS needs to be modified.

QUAN(6,1)=PINT

If no DBMS:

QUAN(6,1)=PRET+PINT

PRET - programming time to permit retrieval of all the data on a specified individual if no data base management system (DBMS) is used.

PINT - programming time to produce a copy of all the information relating to a specified individual in comprehensible form.

Table 5. Requirement 3, Access to Records

Compliance Steps		Actions Necessary to Accomplish Compliance Step
8. Accommodate Record Existence Inquiry		NONRECURRING
	A27	- Develop software to permit retrieval of subject information QUAN(6,1)
		RECURRING
	A28	- Maintain software QUAN(6,6)
	A29	- Utilize clerical effort to process inquiries QUAN(6,14)
	A30	- Operate computer to access and copy the data QUAN(6,9)
	A31	- Mail responses QUAN(6,11)
9. Accommodate Data Accuracy Inquiry		RECURRING
	A32	- Utilize executive time to evaluate data subject claims QUAN(10,13)
10. Store Subject Claims		RECURRING
	A33	- Utilize clerical time to prepare and enter a claim QUAN(11,14)
	A34	- Operate computer storage to hold subject claims QUAN(11,7) or (11,8)

A-28. Software Maintenance (QUAN(6,6))

$$QUAN(6,6) = PRGMNT*QUAN(6,1)$$

A-29. Clerical (QUAN(6,14))

$$QUAN(6,14)=HINQ*NREI$$

HINQ - the amount of clerical time required to process an inquiry and subsequent clerical tasks.

FREI - the percentage of records in the system that will be subject to record existence inquiries per year.

NREI - number of record existence inquiries received per year.

$$NREI=FREI*NREC$$

A-30. Computer (QUAN(6,9))

$$QUAN(6,9)=250*GET+NREI*TCPU*IINT$$

IINT - computer time to access data and print a comprehensible copy.

$$\begin{matrix} (N) & (R) & (L) & (Q) \\ GET(ONLN, & NREC, & SREC, & (.004*NREI)) \end{matrix}$$

It is assumed that inquiries of this type will be batched and processed on a daily basis. This accounts for the factors of 250 and .004 that appear in these equations.

A-31. Mailing Effort (QUAN(6,11))

$$QUAN(6,11)=NREI$$

2.3.2 Compliance Step 9

The agency must be able to respond to data accuracy disputes; they must have the machinery to adjudicate disputes concerning data accuracy.

2.3.2.1 One action (A-32) is required.

A-32 Recurring - Executive time must be utilized to determine the validity of a subject's claim.

2.3.2.2 One algorithm is required:

A-32 Executive time (QUAN(10,13))

$$QUAN(10,13) = NDAI*HJDG$$

HJDG - the number of hours required to receive and act on one data accuracy inquiry.

2.3.3 Compliance Step 10

If the dispute is not resolved, the agency must store the subject's claim.

2.3.3.1 Two actions (A-33 - A-34) are necessary.

A-33. Recurring - The agency must utilize clerical time to prepare and enter claims.

A-34. Recurring - Computer storage must be used to hold claims.

2.3.3.2 Algorithms

A-33. Clerical time (QUAN(11,14))

$$QUAN(11,14) = HPCL*NUDS$$

HPCL - the time needed to prepare and enter one subject's claim.

FRDS - the percentage of data accuracy inquiries that will not result in the addition of a claim to the data base.

NUDS - the number of data accuracy inquiries that are not settled and must be added to the data base per year.

$$NUDS=(1-FRDS)*NDAI$$

A-34. Computer storage (QUAN(11,8) if online)

(QUAN(11,7) if offline)

$$QUAN(11,8) \text{ or } QUAN(11,7)=NUDS*TRRT*SCLM$$

2.4 Requirement 4 - General Agency Requirements

Requirement e of the Privacy Act covers a number of requirements of varying types, dealing with record accuracy, physical security, training, audit, and public notice.

Each agency shall....

(1) Maintain...only such information about an individual as is relevant to accomplish a purpose of the agency required to be accomplished by statute or by executive order.
(2) Collect information to the greatest extent practicable directly from the subject when the information may result in adverse determinations.
(3) Inform each individual on the form which it uses....
  (A) the authority...which authorizes the solicitation of the information and whether (it) is mandatory or voluntary.
  (B) the principal...purposes for which the information is to be used.
  (C) the routine uses which may be made of the information...
  (D) the effects on him...of not providing all or any part of the...information
(4) Publish in the Federal Register at least annually a notice of the existence and character of such records, which notice shall include:
  (A) the name and location...
  (B) the categories of individuals..maintained
  (C) the categories of records
  (D) each routine use
  (E) policies and practices regarding storage, retrievability, access controls, retention, and disposal.
  (F) the title and...address of the agency official responsible...
  (G) agency procedures concerning inquiries...
  (H) the categories of sources of records...
(5) Maintain all records...with such accuracy...as is reasonably necessary to assure fairness to the individual.
(6) Prior to disseminating any record...make reasonable efforts to assure records are accurate.
(7) Establish rules of conduct for persons involved in the development, operation...of any system of records.
(8) Establish physical safeguards.
(9) Publish...notice of any new use of the information in the system.

Table 6. Requirement 4, General Agency Requirements

Compliance Steps	Resources Necessary to Accomplish Compliance Steps
11. Maintain Data Accuracy	NONRECURRING A35 - Develop software to check verification accuracy data-QUAN(8,1) RECURRING A36 - Maintain software-QUAN(8,6) A37 - Utilize clerical time to verify old records-QUAN(8,14) A38 - Operate computer to store verification dates-QUAN(8,8) or (8,7) A39 - Possible saving of storage from elimination of obsolete data-QUAN(8,8) or (8,7)
12. Provide Additional Data if Necessary	RECURRING A40 - Utilize clerical time to obtain data-QUAN(9,14) A41 - Operate computer to store additional data items-QUAN(9,8) or (9,7)
13. Design Forms for Data Supply Obligation Notification	NONRECURRING A42 - Redesign data collection forms-QUAN(1,2) A43 - Establish initial inventory levels of forms-QUAN(1,5)
14. Provide Physical Security	NONRECURRING A44 - Utilize management time to develop a physical security plan-QUAN(17,2) A45 - Utilize management time to develop an audit plan for physical security-QUAN(17,4) A46 - Procure physical security equipment-QUAN(17,5) RECURRING A47 - Utilize manpower to carry out security plan-QUAN(17,14)
15. Provide User Training	NONRECURRING A48 - Train personnel-QUAN(18,3) A49 - Utilize management effort for training of personnel and users-QUAN(18,2) RECURRING A50 - Conduct periodic refresher training required by personnel-QUAN(8,14) A51 - Conduct periodic management effort for refresher training of personnel and users-QUAN(18,13)
16. Audit for System Assurance	NONRECURRING A52 - Develop software to support audit compliance program-QUAN(19,1) + QUAN(19,4) RECURRING A53 - Maintain software-QUAN(19,6) A54 - Operate computer to run audit programs-QUAN(19,9) A55 - Utilize audit manpower to run audit program-QUAN(19,15)
17. Issue Public Notice	RECURRING A56 - Utilize executive time to prepare annual notice for Federal Register-QUAN(20,13)

Seven compliance steps are necessary to accommodate these requirements: Compliance Steps 11-17

11. The agency should develop procedures to keep personal data bases accurate. Periodic updating procedures may be necessary.

12. The agency should review its data to insure that data is complete. If not, additional data should be added.

13. All data collection forms must state the reasons and requirements for collecting data. Redesign may be necessary.

14. Physical security of records must be maintained.

15. Training programs must be prepared and carried out to insure agency personnel comply with the Act.

16. Personal data systems should be periodically audited for compliance.

17. Public notice concerning uses and contents of data bases must be published.

2.4.1 Compliance Step 11

Agencies should develop procedures to keep personal data bases accurate. Periodic updating may be necessary.

2.4.1.1 Five actions (A-35 - A-39) are required for this compliance step.

A-35. Nonrecurring - Develop software to check verification accuracy date.

A-36. Recurring - Maintain software.

A-37. Recurring - Reverify old records.

A-38. Recurring - Operate computer to store verification dates.

A-39. Recurring - Determine storage saving by purging old records.

2.4.1.2 Algorithms

A-35. Software (QUAN(8,1))

QUAN(8,1)=PCVD*(1+0.1*(NRPR-1))

PCVD - the amount of programming time to implement the verification date check in one record retrieval program.

A full programming effort will be required for the first application program. Insertion in other retrieval programs will only require 10% of the original effort. The 10% value may be varied in a sensitivity analysis.

A-36. Maintenance (QUAN(8,6))

QUAN(8,6)=PRGMNT*QUAN(8,1)

A-37. Reverification (QUAN(8,14))

QUAN(8,14)=HVER*FVER*(NREC/TVAL)/2

HVER - clerical effort to reverify one record.

FVER - the percentage of records expiring each year that are reverified.

TVAL - the number of years that information can be considered valid.

Since personal data systems have been growing, the present number of records divided by "record valid life" will probably give too large a number of records to be reverified. Accordingly, NREC/TVAL is divided by two.

A-38 and A-39. Storage & Purging (QUAN(8,8) if online)

(QUAN(8,7) if offline)

QUAN(8,8) or QUAN(8,7) = 4*NREC-(SREC*(1.-FVER)*(NREC/(2*TVAL)))

If records have expired, it may be decided to purge these records rather than reverify them. If this occurs, storage space may become available. The first section, 4*NREC, reflects an additional 4-character field in each record to indicate the date at which it must

be revalidated if it is to continue to be used. The remainder represents the potential reduction in storage due to purging out-of-date records rather than revalidating them. Division by 2 is for the same reason given when discussing clerical revalidation effort above.

2.4.2 Compliance Step 12

The agency should review its data to insure that data is complete. If not, additional data should be added.

2.4.2.1 Two actions (A-40 - A-41) are necessary for this compliance step.

A-40. Recurring - Utilize clerical time to obtain data.

A-41. Recurring - supply complete storage for additional data items.

2.4.2.2 Algorithms

A-40. Clerical (QUAN(9,14))

$$QUAN(9,14) = HCAD*NADY$$

FADY - the fraction of records to which additional data will be added each year.

NADY - the number of additional data fields added to the system per year.

$$NADY=FADY*NREC$$

HCAD - clerical time to obtain and enter one item of additional data.

A-41. Storage (QUAN(9,8) if online)

(QUAN(9,7) if offline)

$$QUAN(9,8) \text{ or } QUAN(9,7) = NADY*TRRT*SADD$$

SADD - the amount of storage space that would have to be allocated for each occurrence of an additional data field.

2.4.3 Compliance Step 13

All data collection forms must state the reasons and requirements for collecting data. Redesign may be necessary.

2.4.3.1 Two action steps (A-42 - A-43) are necessary.

A-42. Nonrecurring - Redesign of data collection forms.

A-43. Nonrecurring - Establishment of initial inventory levels for forms.

2.4.3.2 Algorithms

A-42. Forms redesign (QUAN(1,2))

$$QUAN(1,2) = HFRM*(1+0.2*(NFRM-1))$$

HFRM - manhours required to redesign a form

NFRM - the number of distinct data collection forms used by the personal data system.

It is assumed that redesign of all forms except the first will need only 20 percent of the effort required for the first form.

A-43. Initial Stock Levels (QUAN(1,5))

$$QUAN(1,5) = NFRM*QFRM*.015$$

QFRM - supply level for each form.

Each form is assumed to cost $.015. This parameter may be varied.

2.4.4 Compliance Step 14

Physical security of records must be maintained.

2.4.4.1 Four actions (A-44 - A-47) are required.

A-44. Nonrecurring - Management must develop and implement a physical security plan.

A-45. Nonrecurring - Management must develop an audit plan for physical security.

A-46. Nonrecurring - Physical security equipment must be obtained.

A-47. Recurring - Manpower effort must be utilized to carry out the security plan.

2.4.4.2 Algorithms

A-44 and A-45. Physical Security Plan (QUAN(17,2)) and Audit Security Plan (QUAN(17,4))

QUAN(17,2) = .25* HSPL

QUAN(17,4) = .75*HSPL

HSPL - time required to develop a physical security plan and audit procedures.

It is assumed that 25 percent of development time for a security plan will be borne by agency executives and 75 percent of the time will be borne by agency audit personnel.

A-46. Equipment (QUAN(17,5))

QUAN(17,5)=KSEC

KSEC - the dollar value of additional equipment needed to achieve an appropriate level of security.

A-47. Manpower (QUAN(17,14))

QUAN(17,14)=HGRD

HGRD - manhours required to guard equipment, check identification, etc.

2.4.5 Compliance Step 15

Training programs must be prepared and carried out to ensure agency personnel comply with the act.

2.4.5.1 Four actions (A-48 - A-51) are required for training.

A-48. Nonrecurring - Initial training of all personnel must be completed.

A-49. Nonrecurring - Management must make an initial effort to prepare training classes and train personnel.

A-50. Recurring - Refresher training must be given to agency personnel.

A-51. Recurring - Management must periodically conduct refresher training classes.

2.4.5.2 Algorithms

A-48. Initial Training (QUAN(18,3))

$$QUAN(18,3)=NCLK*HTRC$$

HTRC - the number of class hours required to train clerical personnel.

NCLK - the number of clerical personnel associated with operation of the system.

A-49. Management Preparation (QUAN(18,2))

$$QUAN(18,2)=(HTRC*NCLK+NUSR*HTRU)/SCLS$$

HTRU - hours required to train users other than agency personnel. It is assumed that the agency maintaining the data base will train other agency users.

NUSR - number of potential users of the system.

SCLS - the size of the training class.

A-50. Recurring Training (QUAN(18,14))

$$QUAN(18,14) = FTR*QUAN(18,3)$$

FTR - the frequency of retraining.

A-51. Periodic management time for refresher courses (QUAN(18,13))

$$QUAN(18,13) = FTR*QUAN(18,2)$$

2.4.6 Compliance Step 16

Personal data systems should be periodically audited for compliance.

2.4.6.1 Four action steps (A-52 - A-55) are necessary.

A-52. Nonrecurring - Develop software to support audits.

A-53. Recurring - Maintain software.

A-54. Recurring - Operate computer to run audit programs.

A-55. Recurring - Utilize audit manpower.

2.4.6.2 Algorithms

A-52. Software (QUAN(19,1) and QUAN(19,4))

QUAN(19,1)=.9*PADT

QUAN(19,4)=.1*PADT

PADT - programming needed to prepare all the programs required by system auditors.

It is assumed that auditors must interface with the system programmers to insure an adequate set of audit programs.

A-53. Software Maintenance (QUAN(19,6))

QUAN(19,6) = PRGMNT*QUAN(19,1)

A-54. Computer Time (QUAN(19,9))

QUAN(19,9)=TADT

TADT - the amount of computer time required per year to support the system auditor.

A-55. Audit Manpower (QUAN(19,15))

QUAN(19,15)=PRGMNT*QUAN(19,4)+HADT

HADT - Manhours per year of audit time to assure compliance with the Privacy Act.

Note inclusion of software maintenance in QUAN(19,15).

2.4.7 Compliance Step 17

Public notice concerning uses and contents of data bases must be published.

2.4.7.1 One action (A-56) is required.

A-56. Recurring - utilize executive time to publish annual notice.

2.4.7.2 Algorithm

A-56. Executive time (QUAN(20,13))

QUAN(20,13)=40

40 - It is assumed this action will take 40 hours. This number may be varied in a sensitivity analysis.

3. Summary

Our methodology for defining implementation strategies for complying with the Privacy Act of 1974 is based upon estimating incremental compliance costs for individual personal data system.

The procedure is to first isolate and group the relevant language of the Privacy Act into four general requirements. Second, compliance steps are identified for each requirement. Third, actions are identified for each compliance step. Finally, algorithms are developed for each action. Redundancy between algorithms is factored out and the algorithms are combined into a computer model. We have identified four Requirements, 17 Compliance Steps, and 56 Actions.

The model can be thought of as consisting of two parts. The first part accepts inputs about the personal data system under study, and the algorithms provide incremental resources required to comply with the Privacy Act of 1974. The second part applies cost factors to the resources to provide a cost estimate to bring the personal data system under study in compliance. Both one time (nonrecurring) costs and ongoing (recurring) costs are provided.

A critical factor in effectively implementing our methodology is rendering informed judgment, analysis, and review for the input parameters.

Application of our structured methodology has proved effective in the analysis of proposed privacy regulations for personal data bases in the private sector, and for analysis of the Privacy Act of 1974 for personal data bases in the public sector.

Appendix 1

Glossary of FORTRAN Variables

APPP - Cost of applications programming.

AUDT - Cost of auditor time.

CLAS - Characterization of system.

CLER - Cost of clerical time.

CLINT - If there is a clerical intermediary in obtaining personal data, CLINT=T, if not CLINT=F.

DMS - A logical variable DMS=1 if a DBMS exists, 0 if it does not. A DBMS negates the requirements for PRET.

EXEC - Executive costs.

FADY - The percentage of records to which additional data will be added each year.

FDAI - The percentage of individuals making a record existence inquiry who challenge something in their record.

FDTR - Cost of fast data transmission (Telecommunication).

FOBJ - The percentage of data subjects who may be expected to object to a proposed new use for their information. If a subject objects, his record must be so annotated and blocked from use.

FMRS - Cost of fast (Online) machine readable storage.

FRDS - Frequency of data accuracy disputes resolved in agency's favor.

FREI - The percentage of records in the system that will be subject to record existence inquiries per year.

FRPT - The percentage of NSUB which will require follow-up letters to obtain consent.

FRUI - Frequency of record usage inquiry.

FVER - The percentage of records expiring each year that are reverified.

GET - GET is a function used by several of the algorithms to determine the time necessary to get a record from the file. There are four items used by the GET function (N,R,L,Q).

N = T if the data base is online. If this is true, GET = .14 . This parameter may be varied when it is necessary.

N = 0 if offline

R = Number of records in file

L = Length of a record

Q = Number of records to be retrieved

If Q is less than or equal to one, one half the file must be read and access equals

GET = R*L*1/120,000/2

If Q is greater than 1 and N = 0, the entire file must be read and

GET = R*L*1/120,000/Q

The GET function is based on the following assumptions about file organization and usage:

Online data bases are assumed to be organized using the Indexed Sequential or equivalent method. Access to a single record, at random, will then require, on average, four disc accesses. A time of 35 milliseconds per access is used as being reasonably typical of today's high performance disc systems.

Offline files are assumed to be stored on tape using technology that permits reading the tape at a rate of 120,000 characters per second. If only one record is to be retrieved, one half the file must be read, on the average. If more than one record is to be retrieved during a single search, it is assumed that the entire file will be read and the total time allocated equally among all the records retrieved. 1/120,000 is the amount of time to read one character in the file.

HADT - Manhours per year of audit time to assure compliance with the Privacy Act.

HCAD - Clerical hours to obtain and enter one item of additional data.

HFRM - Manhours required to redesign a form.

HGRD - Manhours required to guard equipment, check identification, etc.

HGSN - Clerical hours to process a legal response.

HINQ - Clerical hours required to process an inquiry and subsequent clerical tasks.

HJDG - The number of hours required to receive and act on one data accuracy inquiry.

HPCL - The hours needed to prepare and enter one subject's claim.

HTRC - Number of class hours necessary to train clerical personnel.

HSPL - Hours required to develop a physical security plan and audit procedures.

HUID - The number of hours of clerical time required to confirm the identity of a person submitting an inquiry.

HTRC - Hours required to train operators in security and privacy.

HTRU - Hours required to train users other than agency personnel. It is assumed that the agency maintaining the data base will train other agency users.

HVER - Clerical hours to reverify one expiring record.

IFRM - The number of CPU instructions to format a request to data subjects.

IINT - Number of instructions to generate a comprehensive hardcopy of records.

ISCN - Instructions to read next record.

ISRC - Personal data from subject.

ISTR - A logical variable whose value is true if the system primarily processes structured inquiries and false if inquiries are primarily unstructured. Unstructured inquiries require greater amounts of transaction processing time.

IWAC - The number of CPU instructions to write control access information.

IWUL - Number of CPU instructions to write data in usage log.

KLOG - The annual dollar cost of additional equipment needed to maintain the usage log.

KSEC - The dollar value of additional equipment needed to achieve an appropriate level of security.

NADY - The number of additional data fields added to the system per year.

NADY=FADY*NREC

NCHK - Number of existing ("Old") records checked each year.

NCLK - The number of clerical personnel associated with operation of the system.

NDAI - Number of data accuracy inquiries per year.

NDRP - The number of application programs which directly access the data base. NDRP=1 if a general data management system is used to handle all requests for data by applications programs.

NFRM - The number of distinct data collection forms used by the personal data system.

NLGS - The frequency of searching the usage log per year.

NLPN - The number of legally enforceable requests for data received per year.

NNSB - Number of new subjects added to file per year.

NNUS - Number of new uses for the data base each year.

NREC - Total number of data subject records. It may be greater than NSUB as one individual may have more than one record in the data base.

NREI - Number of record existence inquiries received per year.

NREI=FREI*NREC

NRLC - The number of record level access control fields per record.

NRPR - The number of record retrieval programs utilizing the data base.

NRUI - Number of record usage inquiries per year.

NSUB - The number of individuals about whom identifiable personal data is stored in the system.

NTRN - The average number of transactions processed by the system per year.

NUDS - The number of data accuracy inquiries that are not settled and must be added to the data base per year.

NUDS=(1-FRDS)*NDAI

NUSR - Number of potential users of the system.

NUST - The number of sets into which all users can be lumped for access control purposes.

ONLINE - ONLN

ONLN - If the data base is online, ONLN=1. If the data base is offline, ONLN=0.

OPS - Variable which = 300 if system inquiries are unstructured and 100 if inquiries are structured. Used with ISTR. Unstructured inquiries are assumed to require three times as much processing time as structured inquiries.

PACC - Programming hours to implement record level access control.

PADT - Programming hours needed to prepare all the programs required by system auditors.

PCVD - The amount of programming hours to implement the verification date check in one record retrieval program.

PDCL - The programming hours to modify a record retrieval program to include the claim field in its response to all inquiries.

0.1* (PDCL) - The additional hours necessary to modify subsequent retrieval programs after the first program has been modified.

PINT - Programming hours to produce a copy of all the information relating to a specified individual in comprehensible form.

PLOG - The amount of programming hours required to implement the usage log capability.

PNOT - The amount of programming hours necessary to generate a program for writing form letters to all data subjects.

PRET - Programming hours to permit retrieval of all the data on a specified individual if no data base management system (DBMS) is used.

PRGMNT - The percentage of initial programming hours required annually for program maintenance.

PRSB - Print subject's file in "comprehensible" form.

PUID - The programming hours required to add a user identification to the system.

PWAC - The amount of programming hours necessary to generate a program to permit the recording of all access control information within the data base and within each subject's record.

QFRM - Inventory level of each form on hand.

QUAN(i,j) - An array used for programming and convenience. The i subscript relates to the compliance step. The j subscript relates to the type of resource.

i Values

1. Data Supply Obligation Notification
2. Consent for Additional Use
3. Check Usage Authorization
4. Usage Log Maintenance
5. Record Existence Notification (not required by 1974 Privacy Act)
6. Record Existence Inquiries
7. Record Usage Inquiries
8. Data Accuracy
9. Additional Data
10. Data Accuracy Inquiries
11. Subject Claim Storage
12. Subject Claim Dissemination
13. Retroactive Claim Dissemination
14. Record Transmission (not required by 1974 Privacy Act)
15. Consent to Transfer Date (not required by 1974 Privacy Act)
16. Legal Process Notification
17. Physical Security
18. User Training
19. System Assurance
20. Public Notice

j Values

1. Programming (Conversion)
2. Executive Time (Conversion)
3. Clerical Time (Conversion)
4. Auditor Time (Conversion)
5. Capital Expenditure (Conversion)
6. Programming (Annual)
7. Offline Machine Readable Storage (Annual)
8. Online Machine Readable Storage (Annual)
9. Schedulable Computer Processing (Annual)
10. Real Time, Online Computer Processing (Annual)
11. Slow Data Transmission (Annual)
12. Fast Data Transmission (Annual)
13. Executive Time (Annual)
14. Clerical Time (Annual)
15. Auditor Time (Annual)
16. Capital Expenditure (Annual)

RTPR - Cost of instantaneous processing.

SADD - The amount of storage space in characters that would have to be allocated for each occurrence of an additional data field.

SANS - Size of average inquiry answer in characters.

SCLM - Characters needed to express one subject's claim.

SCPR - Cost of schedulable processing.

SDTR - Cost of slow data transmission (U.S. Mail).

SLOG - Size of log entry.

SMRS - Cost of slow (Batch) machine readable storage.

SYSP - Cost of systems programming.

TADT - The amount of computer hours required, per year, to support the system auditor.

TCPU - Time in seconds required to execute 1 instruction.

TLGR - Length of time an entry is maintained in the usage log in years.

TTRN - The computer time in seconds needed to process one transaction.

TTRN=OPS*SANS*TCPU

TRRT - Number of years a record is retained.

TVAL - The number of years that information can be considered valid.

XG - If agency is exempt due to law enforcement XG=T, if not, XG=F.

XS - If agency is exempt for other reason XS=T, if not, XS=F.

Appendix 2

Patterned Interview Format for Data Gathering

1. This appendix contains the questions used to obtain the data base attributes necessary to use the algorithms in Section 2. The specific datum is listed below the question.
2. Questions without a specific datum are general in nature and are used to get general information concerning the data base. The general information is useful in reviewing those assumptions implicit in the structure of the model.

Data Collection

Section I: System Attributes

1. Which of the following application areas best characterizes your system? (If more than one applies, please indicate the most important one, and answer all remaining questions with respect to just that part of your total system.)

..... Credit

..... Education

..... Employee (Not a program input)

..... Health

..... Insurance

..... Law Enforcement

..... Welfare

..... Other (Please specify:.....CLAS.....)

2. How many individuals are subjects of identifiable information in your system?

NSUB

Number of individuals

3. How many separate records does the system contain? (Some systems may be organized with more than one record per individual.)

NREC

Number of records

4. How many new individuals are added to the system in an average year?

NNSB (Not a program input)

Number of individuals

5. For how long are records retained within the system?

..TRRT....

Number of Years

6. For how long (on the average) is data about an individual valid for its intended use?

..TVAL....

Number of Years

7. Is there a regular program of periodically revalidating information?

Yes or No (Not a program input)

8. If so, how many "old" records are re-checked each year?

..NCHK....

Number of Records

9. What is the average size of a record (in characters)?

SREC

Number of Characters

10. How many individuals are potential users of your system; that is, how many may initiate transactions?

NUSR

Number of Individuals

11. If these users can be lumped into sets for access authorization purposes, how many such sets are there?

..NUST....

Number of Sets

12. How many individuals are involved in the operation of your system including data entry and other clerical tasks?

NCLK

Number of Individuals

13. Are inquiries made:

CLINT=F directly by the person wanting the information, or

CLINT=T by a clerical intermediary?

14. How many transactions are processed per year (on the average)?

NTRN

Number Transactions/Year

15. Are transactions processed:

ONLINE=T interactively, or

ONLINE=T using online batch techniques, or

ONLINE=F offline?

16. Does your system permit:

ISTR=F only specific, highly structured queries, or

ISTR=T unstructured browsing?

17. How many transaction processing programs exist in your system?

NRPR

Number of Programs

18. Do transaction processing programs access the data base:

.DMS. directly, or

..... through a general purpose data management program?
If so, which one?.....

19. What is the average size (in characters) of the answer your system provides to a query?

..SANS.....

Characters

20. How many different data collection forms do you use?

..NFRM.....

Number of Forms

21. How many copies of each data collection form are normally on hand?

..QFRM.....

Number in Stock

22. How many times per year do you receive a legally enforceable request to supply data about an identifiable individual?

..NLPN....

23. Does most personal data in your system come from:

ISRC=T the subject, himself, or

ISRC=F someone else?

24. What computer model(s) is (are) used to run this system?

List Computers.

(Not a Program Input)

25. Is your system accurately described by the following:

"a system of records maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws."

XG

Yes or No

Yes = T
No = F

26. Is your system accurately described by the following:

"a system of records--

(1) of investigatory material compiled for law enforcement purposes (other than those described in the preceding question);

(2) maintained in connection with providing protecting services to the President;

(3) used solely as statistical records;

(4) compiled solely for the purpose of determining eligibility for Federal civilian employment, military service, Federal contracts, or access to classified information;

(5) of testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service;

(6) evaluation material used to determine potential for promotion in the armed services.

XS

Yes or No

Yes = T
No = F

Section II: Resource Prices

This section asks you to estimate the unit costs to your organization of various information processing resources. Please include in your estimates any overheads or other indirect costs that may be associated with each item. DON'T FORGET TO STATE YOUR UNITS FOR EACH ANSWER. If costs are difficult to determine, can you supply numbers of people involved or other indicators of cost.

27. Sequential-access, machine-readable storage - i.e., magnetic tape or punched cards:

...SMRS...

$/Character/Yr.

28. Random-access, machine-readable storage - i.e., magnetic disks or drums, or bulk core:

...FMRS...

$/Character/Yr.

29. Schedulable computer processing - that is, processing which may be preplanned for convenient times:

...SCPR...

$/Sec.

About what percentage of total computer processing is schedulable?

..... (Not a Program Input)

30. Non-schedulable computer processing - that is, processing which must be performed instantly when demanded:

...RTPR...

$/Sec.

Percentage of total processing non-schedulable:

..... (Not a Program Input)

31. Slow data transmission - i.e., U. S. Mail:

...SDTR...

$/Doc.

32. Fast data transmission - via communications lines:

FDTR
.....

$/Character

33. Systems programming - including related computer time and other support

...SYSP...

$/Hour

How many people?

..... (Not a Program Input)

34. Applications programming - including computer and other support:

...APPP...

$/Hour

How many people?

..... (Not a Program Input)

35. Administration - policy creation and review, training, enforcement of regulations:

...EXEC...

$/Hour

How many people?

..... (Not a Program Input)

36. Clerical processing - data entry, filing, handling inquiries:

...CLER...

$/Hour

How many people?

..... (Not a Program Input)

37. Audit - system performance monitoring - quality control

...AUDT...

$/Hour

How many people?

..... (Not a Program Input)

Section III: Sizes

These questions refer to the amount of computer storage space that would be required to hold various items of information.

38. The size of the field that would be required to hold one item of "additional data". "Additional data" is information that is not currently part of a record but which may be considered necessary to a proper interpretation of the record. Examples would include the ultimate disposition of an arrest or the fact that an unpaid bill is disputed.

...SADD...

Number of Characters

39. How many times per year would you expect to add such an item of "additional information" to a record?

...NADY...

Times/Yr. (Cross Check Only, NADY Computed By Program)

40. The number of characters of storage that would be allotted to store the dissenting opinion of a data subject:

...SCLM...

Number of Characters

41. The size of an entry in the record usage log. This entry must contain the date and purpose of the access and the identity of the individual and organization making the inquiry:

...SLOG...

Number of Characters

42. What retention time do you think is appropriate for record usage information?

..... (Not a Program Input)

43. The number of computer instructions that would be executed to generate a usage log entry is:

...IWUL...

Number of Instructions

44. The number of computer instructions that would be executed to reference the "next" record in a sequential scan of the entire file is:

...ISCN... (Already in Program)

Number of Instructions

45. The number of computer instructions that would be executed to generate a hardcopy of all the information relevant to a specific individual is (not counting the time needed to locate and access the information):

...IINT...

Number of Instructions

46. The amount of computer time required for auditing and program verification purposes is:

...TADT...

Number of Hours

Section V: Man-hours

These questions deal with the amount of human time, administrative or clerical, required to perform the specified functions.

47. How many man-hours of auditing time per year would be required to assure that the system was in compliance with the Privacy Act?

...HADT...

Number Hours/Yr.

48. How many man-hours of administrative time would be required to redesign each data collection form to include the appropriate notices to potential data subjects?

...HFRM...

Hours/Form

49. How many man-hours of administrative time would be needed to develop an appropriate set of security policies?

...HSPL...

Hours

50. How many man-hours of administrative time would be needed to evaluate and reach a decision on a data subject's complaint about the validity of his record?

...HJDG...

Hours

51. How many man-hours of clerical time would be needed to prepare and enter a subject's claim concerning his record?

...HPCL...

Hours

52. How many man-hours of clerical time would be required to generate a notification to a data subject?

...HGSN...

Hours

53. How many man-hours of clerical time would be needed to accept and process a subject's inquiry concerning his record?

..HINQ....

Hours

54. How many man-hours per year would have to be devoted to security related tasks such as guarding equipment and data, and checking personnel identification? (see additional checklist)

..HGRD....

Hours

55. How long would it take to manually verify the identity of an individual submitting a transaction offline?

HUID
.....
Hours

56. How many man-hours would be required (on the average) to collect a required item of "additional data"?

...HCAD....

Hours

57. How many man-hours would be required to reverify the accuracy and timeliness of an old record?

...HVER....

Hours

58. How many hours of training in security and privacy policies and procedures would be required for each person involved in the operation of your system?

...HTRC....

Hours

59. How many hours of training in security and privacy policies and procedures would be required for each user of the system?

...HTRU...
Hours

Are you responsible for this training? .....

Section VI: Programming Time

A number of proposed privacy regulations would appear to require the modification of existing data handling programs, and in some cases, the creation of entirely new ones. These questions are designed to get at the amount of work required to accomplish this. If your system already includes a capability listed below, please so indicate.

How many man-hours of programming time (including program design, coding, testing and documentation) would be required to:

60. Support the system auditing function:

PADT .....

Total Hours

61. Enable the operating system to check and confirm the identity of a user:

PUID .....

Total Hours

62. Enable the generation of a notice to each data subject:

PNOT .....

Total Hours

63. Permit checking the authorization of each access on the basis of user identification and stated purpose:

PWAC .....

Total Hours

64. Include the capability for checking the "verification date" field each time a record is retrieved, and keeping a list of records older than a specified date:

PCVD .....

Total Hours

65. Provide for the "subject's claim" field in each record and ensure that it is included with all responses from an individual's record:

..PDCL....

Total Hours

66. Implement the usage log, including the creation, storage, and retrieval of usage records:

..PLOG....

Total Hours

67. Retrieve all of the data relevant to a particular individual:

..PRET....

Total Hours

68. Print an individual's record in "comprehensible" form:

..PINT....

Total Hours

69. Provide for the adding or removal of entries in a record's access control field?

..PACC....

Total Hours

Section VII: Counts

This section asks for estimates of a few miscellaneous numbers.

70. The number of times per year that a new application might be expected to be added to the system is:

...NNUS...

New Applications/Yr.

71. The fraction of mailed requests to data subjects that would have to be repeated because the subject failed to respond the first time is:

...FRPT...

Percent

72. The dollar value of additional hardware required to maintain the usage log is:

...KLOG...

Total Dollars

73. The dollar value of additional hardware needed to provide system and data security is:

...KSEC...

Total Dollars

74. Does your organization send a regular mailing (at least once a year) to all data subjects?

Yes or No. (Not a Program Input)

75. What is your estimate of the fraction of the initial programming cost of a system that is expended annually for ongoing maintenance of that system?

...FMNT... PRGMNT

Percent

76. What fraction of the data subjects of this system would you expect to refuse permission to have their records used for some new purpose?

...FOBJ...

Percent

77. What fraction of the data subjects of this system would you expect to enquire (per year) about the existence and content of their records?

...FREI...

Percent

78. Of those data subjects enquiring about the contents of their record, what fraction would you expect to enquire about the usage made of the record?

...FRUI...

Percent

79. Of those data subjects enquiring about the contents of their record, what fraction would you expect to dispute some aspect of the record?

...FDAI...

Percent

80. What fraction of the disputes concerning an individual's record would you expect to be settled through a review procedure?

...FRDS...

Percent

Comments, suggestions, and questions should be addressed to:

John L. Berg
Privacy Model
Systems and Software Division
Room A-265, Building 225
National Bureau of Standards
Washington, D.C. 20234

Machine-readable copies of the Privacy Model Computer Program are available through the National Technical Information Service

USCOMM-NBS-DC

NBS-114A (REV. 7-73)

U.S. DEPT. OF COMM. BIBLIOGRAPHIC DATA SHEET	1. PUBLICATION OR REPORT NO. NBS TN-906	2. Gov't Accession No.	3. Recipient's Accession No.

4. TITLE AND SUBTITLE

A Methodology for Evaluating Alternative Technical and Information Management Approaches to Privacy Requirements

5. Publication Date June 1976

6. Performing Organization Code

7. AUTHOR(S)

Robert C. Goldstein, Henry H. Seward, Richard L. Nolan

8. Performing Organ. Report No.

9. PERFORMING ORGANIZATION NAME AND ADDRESS

D. P. Management Corporation
1 Militia Drive
Lexington, Mass. 02173

10. Project/Task/Work Unit No. 640.1117

11. Contract/Grant No. 5-35935

12. Sponsoring Organization Name and Complete Address (Street, City, State, ZIP)

National Bureau of Standards
Department of Commerce
Washington, D.C. 20234

13. Type of Report & Period Covered Final

14. Sponsoring Agency Code

15. SUPPLEMENTARY NOTES

16. ABSTRACT *(A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here.)*

Cost becomes an early concern in applying privacy safeguards to any computerized record-keeping system. To determine privacy cost impact one requires a concrete and rigorous approach that permits repeated analysis of carefully documented assumptions. Such a methodology appears in the work reported in the book The Cost of Privacy by Dr. Robert C. Goldstein. This report represents the application of that methodology to the technical requirements flowing from the Privacy Act of 1974 (PL 93-579).

The methodology presented reduces the legislation to 17 compliance steps. Each compliance step then decomposes into one or more specific actions required of the record-keeper. The actions, in turn, translate into the expenditure of different resources. The resources, in dollars, are computed by a set of algorithms collectively called a privacy model and implemented as a computer program.

The privacy model contains algorithms reflecting resource expenditures for 56 distinct actions. Written as a FORTRAN program, the model produces several printouts that show the user the consequences of the input data. In addition to a total cost for conversion and an annual operating cost, the model provides sub-total costs for each compliance step. The model's potential uses include the comparison of costs associated with alternative safeguards, the selection of an optimal set of cost-effective safeguards, and the analysis of those factors having the greatest impact on costs.

17. KEY WORDS *(six to twelve entries; alphabetical order; capitalize only the first letter of the first key word unless a proper name; separated by semicolons)*

Computer security; confidentiality; cost model; data security costs; PL 93-597; privacy; Privacy Act of 1974; privacy compliance techniques; privacy costs; privacy model; security costs

18. AVAILABILITY

[X] Unlimited

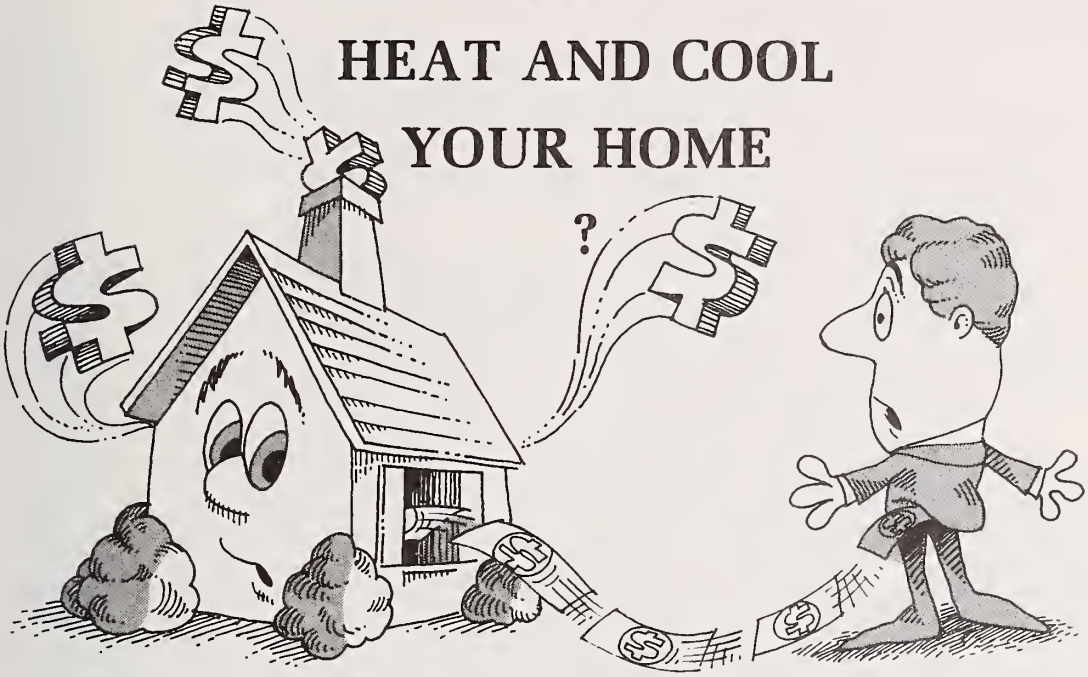
[ ] For Official Distribution. Do Not Release to NTIS

[X] Order From Sup. of Doc., U.S. Government Printing Office Washington, D.C. 20402, SD Cat. No. C13.46:906

[ ] Order From National Technical Information Service (NTIS) Springfield, Virginia 22151

19. SECURITY CLASS (THIS REPORT)	21. NO. OF PAGES
UNCLASSIFIED	72
20. SECURITY CLASS (THIS PAGE)	**22. Price**
UNCLASSIFIED	$1.35

ARE YOU SPENDING MORE TO HEAT AND COOL YOUR HOME

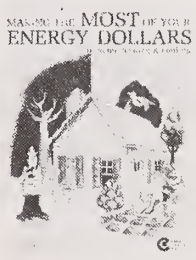


You could be "Making the MOST of Your ENERGY DOLLARS in Home Heating & Cooling"

Making the Most of Your Energy Dollars is a new consumer guide from the Commerce Department's National Bureau of Standards, in cooperation with the Federal Energy Administration.

For your climate and the type of energy used to heat and cool your house, this booklet lets you find your best investment in energy conservation improvements. This investment gives you the greatest possible net savings in your heating and cooling bills over the long run.

Use the booklet to figure out just how much insulation, storm windows and doors, weather stripping and caulking are needed for your house—and what they will cost. Not a how-to-do-it book, but a "how-much" guide to energy conservation investments.



To make the most of YOUR energy dollars send $0.70 per copy (check, money order or Superintendent of Documents Coupons) to Consumer Information, Public Documents Distribution Center, Pueblo, Colorado 81009. Ask for *Making the Most of Your Energy Dollars in Home Heating and Cooling.*

U.S. DEPARTMENT OF COMMERCE/National Bureau of Standards
FEDERAL ENERGY ADMINISTRATION / Office of Energy Conservation and Environment

NBS TECHNICAL PUBLICATIONS

PERIODICALS

JOURNAL OF RESEARCH reports National Bureau of Standards research and development in physics, mathematics, and chemistry. It is published in two sections, available separately:

• **Physics and Chemistry (Section A)**

Papers of interest primarily to scientists working in these fields. This section covers a broad range of physical and chemical research, with major emphasis on standards of physical measurement, fundamental constants, and properties of matter. Issued six times a year. Annual subscription: Domestic, $17.00; Foreign, $21.25.

• **Mathematical Sciences (Section B)**

Studies and compilations designed mainly for the mathematician and theoretical physicist. Topics in mathematical statistics, theory of experiment design, numerical analysis, theoretical physics and chemistry, logical design and programming of computers and computer systems. Short numerical tables. Issued quarterly. Annual subscription: Domestic, $9.00; Foreign, $11.25.

DIMENSIONS/NBS (formerly Technical News Bulletin)—This monthly magazine is published to inform scientists, engineers, businessmen, industry, teachers, students, and consumers of the latest advances in science and technology, with primary emphasis on the work at NBS. The magazine highlights and reviews such issues as energy research, fire protection, building technology, metric conversion, pollution abatement, health and safety, and consumer product performance. In addition, it reports the results of Bureau programs in measurement standards and techniques, properties of matter and materials, engineering standards and services, instrumentation, and automatic data processing.

Annual subscription: Domestic, $9.45; Foreign, $11.85.

NONPERIODICALS

Monographs—Major contributions to the technical literature on various subjects related to the Bureau's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NBS, NBS annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

Applied Mathematics Series—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a world-wide program coordinated by NBS. Program under authority of National Standard Data Act (Public Law 90-396).

NOTE: At present the principal publication outlet for these data is the Journal of Physical and Chemical Reference Data (JPCRD) published quarterly for NBS by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements available from ACS, 1155 Sixteenth St. N. W., Wash. D. C. 20056.

Building Science Series—Disseminates technical information developed at the Bureau on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NBS under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The purpose of the standards is to establish nationally recognized requirements for products, and to provide all concerned interests with a basis for common understanding of the characteristics of the products. NBS administers this program as a supplement to the activities of the private sector standardizing organizations.

Federal Information Processing Standards Publications (FIPS PUBS)—Publications in this series collectively constitute the Federal Information Processing Standards Register. Register serves as the official source of information in the Federal Government regarding standards issued by NBS pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

Consumer Information Series—Practical information, based on NBS research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.

NBS Interagency Reports (NBSIR)—A special series of interim or final reports on work performed by NBS for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Service (Springfield, Va. 22161) in paper copy or microfiche form.

Order NBS publications (except NBSIR's and Bibliographic Subscription Services) from: Superintendent of Documents, Government Printing Office, Washington, D.C. 20402.

BIBLIOGRAPHIC SUBSCRIPTION SERVICES

The following current-awareness and literature-survey bibliographies are issued periodically by the Bureau:

Cryogenic Data Center Current Awareness Service

A literature survey issued biweekly. Annual subscription: Domestic, $20.00; foreign, $25.00.

Liquefied Natural Gas. A literature survey issued quarterly. Annual subscription: $20.00.

Superconducting Devices and Materials. A literature survey issued quarterly. Annual subscription: $20.00. Send subscription orders and remittances for the preceding bibliographic services to National Bureau of Standards, Cryogenic Data Center (275.02) Boulder, Colorado 80302.

Electromagnetic Metrology Current Awareness Service Issued monthly. Annual subscription: $24.00. Send subscription order and remittance to Electromagnetics Division, National Bureau of Standards, Boulder, Colo. 80302.

U.S. DEPARTMENT OF COMMERCE
National Bureau of Standards
Washington, D.C. 20234

OFFICIAL BUSINESS

Penalty for Private Use, $300

POSTAGE AND FEES PAID
U.S. DEPARTMENT OF COMMERCE
COM-215

U.S.MAIL

SPECIAL FOURTH-CLASS RATE
BOOK

AMERICAN REVOLUTION BICENTENNIAL 1776-1976

75 YEARS NBS 1901-1976

1298